(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) Internati nal Publication Date
30 November 2000 (30.11.2000)

PCT

(10) International Publication Number
WO 00/72149 A1

(51) International Patent Classification⁷: G06F 11/30, H04L 9/00

(21) International Application Number: PCT/US00/11437

(22) International Filing Date: 28 April 2000 (28.04.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/318,305 25 May 1999 (25.05.1999) US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: GEIGER, Robert, L.; 1675 Teri Lane, Algonquin, IL 60102 (US). PALANISWAMY, Avinash, C.; 7816 Lakewood Drive, Austin, TX 78750 (US).

(74) Agents: BOSE, Romi, N. et al.; Motorola Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

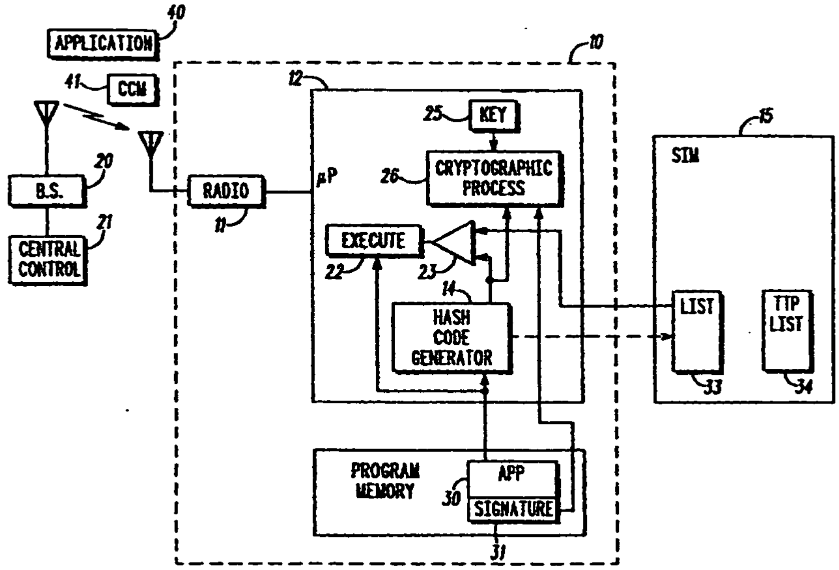
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: PRE-VERIFICATION OF APPLICATIONS IN MOBILE COMPUTING



(57) Abstract: A list of application programs (33) is stored and, for each application program, a digital fingerprint of that application program. Upon execution of an application program, a check (23, 206) is made of the list for an entry that includes the digital fingerprint of the application program. The application is executed if the digital fingerprint is present. Otherwise digital signature verification (26, 220) is performed for the application program if the digital fingerprint is not present in the list.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PRE-VERIFICATION OF APPLICATIONS IN MOBILE COMPUTING

Field of the Invention

This invention relates to verification of application software and applets (generally referred to as applications) prior to running on a processor in a mobile computing environment, for the purposes of insuring that an application is appropriately authorized from a security point of view, whether for system security or other purposes.

Background of the Invention

In the field of software security, it is know to create digital certificates for software applications. A software vendor is provided with an encryption key that permits the vendor to generate a certificate that has a digital signature generated from the encryption key. A user of the software from that software vendor can verify that the software has originated from the authorized vendor by checking the digital signature of the accompanying certificate. The certificate is typically a fixed-length "hash" of the software encrypted with the encryption key. The user is able to verify the signature because the user is provided with an encryption key from the same security domain as the encritypion key of the vendor, i.e. the two encryption keys share the same route key. The user is therefore able to verify that the digital certificate originates from the authorized security domain.

The process of verifying a signature of a digital signature is time consuming. If the signature has to be checked each time an application is launched or each time a new application is downloaded to a mobile device, the process of using the mobile device is degraded in its speed performance. This becomes particularly noticeable if a device is started up and, upon power up, several applications have to be launched and the signatures of all the applications have to be verified. It is a particular need in the mobile computing environment that time to operation upon power-up is minimized. There is a need for a faster method of verifying the authenticity of an application and maintaining security upon application launch, while avoiding the need for lengthy signature verification processes.

There is also a need for an improved manner of enabling and disabling certificates in a mobile device remotely from a mobile communications network in a secure manner.

Brief Description of the Drawings

FIG. 1 is block diagram illustrating a mobile computing device in communications with a mobile communications network.

FIG. 2 is a flow diagram of a process performed by an issuer of a subscriber identity module (SIM).

FIG. 3 is a flow diagram of a process performed in the mobile communications device of Fig. 1.

FIG. 4 is a second program performed by the communications device of FIG. 1, upon receipt of a certification configuration message (CCM).

FIG. 5 is a message format diagram illustrating the format of a CCM message.

Detailed Description of the Drawings

Referring to FIG. 1, a mobile communications device 10 is illustrated comprising a transceiver radio 11, a microprocessor 12 and a program memory 13. Other elements of the mobile communications device 10 are not illustrated but are well known in the art. The communications device 10 has a subscriber identity module (SIM) 15 that is typically in the form of a miniature smart card that slots into a receiving slot in the communications device 10. The radio 11 is in radio communications with a base station 20 that has a central controller 21.

Also illustrated in FIG. 1 in the microprocessor 12 is a hash code generator 14, a program execution process 22, a comparison element 23, an encryption key register 25 and a cryptographic process 26, all implemented in software. Also illustrated is an application 30 stored in the program memory 13. The application 30 has a digital certificate 31 that is a "signed" hash of the application 30. Illustrated in SIM 15 is a list 33 of authorized applications. Further illustrated in FIG. 1 are certain elements of information passing from the base station 20 to the radio 11, including an application 40 and a certification configuration message 41.

In operation, the mobile communications device 10 is powered up and applications are loaded from the program memory 13 into the microprocessor 12. For running of an application, a check is made against the list 33 in the SIM 15 to verify whether the application is authorized for running. New applications 40 can be received over the air from the base station 20 and stored in program memory 13. Configuration change messages 41 can be received from the central control 21 via the base station 20. Other operations and processes are performed that need not be described in detail.

When a subscriber is issued with a SIM 15, a list 33 is generated and loaded in the SIM. The process of FIG. 2 is performed by the entity issuing the SIM to the subscriber.

Upon commencement of the process of FIG. 2 (step 100) a hash is created by a hash code generator (equivalent to hash code generator 14) of any executable object that is to be permitted to be run on the microprocessor 12. This hash is created in step 101 by passing the executable code of the object through a hash generator such as a SHA1 hash generator in a manner known in the art. The hash code generator performs a mathematical one-way function on the executable code that has two properties: 1) from an arbitrary number of bytes, of input, a finite number of bits of output are generated (e.g. 160 bits) whereby virtually no two inputs give the same output and 2) from an output it is not possible to discern the input. The resultant hash code is much shorter than the object itself, but is of sufficient length that is virtually unreproduceable. The creation of a hash of an executable object is also referred to as creation of an executable object "fingerprint". The hash used is of the same type as that used for signing a digital signature of a new object.

In step 102, the hash code is stored in a protected verified application list 33 in the SIM 15. The process of FIG. 2 is executed for every object (application, applet or other object) to be run on the microprocessor 12.

Every time a new application is launched (for example upon power-up of the mobile communications device, or upon launching of a new application after power-up) or upon downloading a new application 40 to the mobile communications device 10, the process of FIG. 3 is executed. Upon the start of the process at step 200, and upon launching of the application or downloading of the applet (step 201), a hash is created of the application or applet in step 202 using the hash generator 14. This hash is again the same hash as would be used for computing the digital signature of the application or applet. In step 204, the hash so created is checked by comparison element 23 against the verified application list 33. If the hash value (digital fingerprint) is present in the list (step 206) and if the entry has not expired (step 208), the application or applet is launched in step 210. As a preferred (but not essential) feature, a counter is decremented (or incremented) for that application or applet in step 212 each time it is executed.

If no list entry for the object is present (step 206) or if the entry for the object has expired (step 208) full signature verification is performed by cryptographic process 26 in step 220. In full signature verification, the hash already created is one of the inputs of the public key cryptographic process 26 that performs processor-intensive cryptography. If the digital signature of the application is successfully verified, the application is executed by execute process 22 in step 210. Optionally, the hash of the application is added to the list 33 (as shown by the dashed line in FIG. 1). If the digital signature is not verified in step 222, the application is not launched and the process ends at step 230, ready for launch of the next application.

It is a preferred feature that there is a maximum number of uses for an entry in the list 33 before that entry is marked invalid by comparison element 23. A preferred value of five uses is suitable. Each time step 212 is executed, the counter (not shown in FIG.1) for that entry is decremented (or incremented) and when the counter reaches zero (or reaches a threshold respectively), step 208 will indicate that the entry has expired when it is next launched. The list 33 preferably has a maximum size and a prioritization scheme is used to determine which applications to delete when the list is full and a new entry is added to the list.

In the event that a new certificate configuration message (CCM, described below) is received by the mobile device 10, all verified application list entries must be marked invalid. Alternately, a mechanism is provided to determine the validity of an authorizing certificate entry for each application in the list.

As a preferred optional feature, a pointer is stored with the application, pointing to the entry in the list for the authorizing certificate. This avoids having to invalidate the entire verified-application list when a new CCM arrives.

Referring now to FIGs. 4 and 5, a process for maintaining a list of third parties certificates is described. A list 34 of trusted third party (TTP) certificates is maintained is the SIM 15 or in the mobile device 10. This list includes the certificates of all third parties that are trusted by the user of the communication device 10. For example, multiple software vendors may be trusted, all authorized by a common root entity in a common security domain, where the root entity is in position of the root key, the trusted third parties certificates are signed with signatures derived from the root key and the TTP list 34 in the mobile device has corresponding digital signatures that it can use to verify the signatures of the TTP certificates.

The list entries in list 34 contain certificate fingerprints in the form of hashes of the encoded sign certificates. The full hash output for the specified algorithm must be used to generate the fingerprint. A list generator checks to insure that no two list entries match when a list is created. For an X509V3 or X9.68 certificate, the fingerprint hash is computed over the ASN.1 encoded signed certificate object, first octet to last octet. For WTLS certificates, the hash is computed over the signed WTLS certificate in network transmission format, first octet to last octet.

The signature type and length are indicated by the administrator certificate, which must be present on the device. If no administrator certificate is on the device or the signature does not verify, the message is rejected.

The process of FIG. 4 commences upon a receipt of a new certification configuration message in step 502. In step 504, a check is performed to check that the CCM is valid. If no administrator certificate is present in the mobile communications device 10 or its SIM 15, or if the administrator certificate signature does not verify with the signature of the CCM 41, the message is rejected in step 506.

Assuming the CCM is valid, the communications device 10 begins a scan through the trusted third certificate party list 34 (step 510). At the beginning of a scan, a counter "n" is set to one (step 512). If, for a given certificate in the TTP list 34, there is no stored fingerprint, a fingerprint for that entry "n" is computed in step 514. In step 516, a check is carried out to check whether a fingerprint for an authorized TTP in the CCM message matches a fingerprint in the TTP list 34. If it does not match, the certificates in the TTP list 34 is disabled in step 518. If the fingerprint stored in the list 34 matches the fingerprint received in the CCM 41, the certificate is enabled in step 520. The scan continues in a simple loop counter manner by checking step 522 whether the counter n has reached its maximum value N. If not, the counter is incremented in step 528 and the next fingerprint is checked (with pre-computation of that fingerprint if necessary). When the last fingerprint in the list has been checked, the process ends at step 530.

The format of a CCM message is illustrated in FIG. 5. The CCM is either periodically fetched from the central controller 21 or downloaded by the central controller 21 to the device 10. The following is a table of the elements illustrated in FIG. 5.

"Version" is the version number of the security specification (e.g. version 1) "certificateAdvice" is enumerated { enable-all (0), disable-all (1), enable-list (2), disable-list (3) }
"listLength" is the total length of the following list and must be sent as zero when certificateAdvice is enable-all or disable-all.
"hashType" is enumerated { md5 (0), sha-1 (1) }
"hashLength" is the number of octets output by the selected hash type (16 for MD5 and 20 for SHA-1).

A record must be kept of the domain that authorized a given application. If a CCM message is received while applications are currently running, a check must be made that any applications no longer in the trusted domain have their permissions reconfigured appropriately.

The format for entry in list 34 is: one octet hashType; 2 octets permissions; and a number of octets of hash value equivalent in length to the hashLength.

There now follows, for completeness, a description of various further aspects of certificate management.

Three type of certificates are provided for: 1.) operator, 2.) manufacturer, and 3.) trusted third party. It is not necessary that all types be present but the operator and manufacturer root certificates must be present for these domains to be enabled. The manufacturer may load initial third party certificates on the device. Further certificates may be downloaded to the device as signed wireless application protocol (WAP) or world wide web (WWW) content. Downloaded certificates must be verified by an existing trusted certificate and are placed in the domain defined by the root certificate at the top of the verification chain for the downloaded certificate. Third party root certificates should be in protected memory. All third party certificates are subject to restrictions imposed by valid certificate configuration messages.

New third party root certificates may be downloaded as signed WAP or WWW content. The signature on the content should be of a device administrator.

The manufacturer root certificate is pre-loaded in protected, preferably read only, memory on the device at manufacture time. The manufacturer should include a mechanism to re-key the device due to key compromise. Since the manufacturer root is preferably in read only memory this can be accomplished by having multiple root certificates stored and switching between them with a proprietary change message.

The operator root certificate is provided on the SIM if support for certificate storage on the SIM exists. For legacy SIMs not having such storage, the operator root may be downloaded using the root download procedure described below.

Certificates below a given root are installed in files using a hierarchical structure corresponding to the structure of the domain. For single level domains this is equivalent to a directory for each domain; multi-level domains require a hierarchical directory structure.

The actions that can be performed for a given certificate are: 1.) addition, 2.) deletion, 3.) mark trusted, 4.) mark un-trusted, 5.) modify fine grain access permissions. The ability to perform these actions depends no the certificate type being modified as well as the access level of the entity performing the operation. Device users may always delete, mark trusted or untrusted, or modify fine grain access permissions for third party certificates. They may add a third party certificate as long as it is certified by an existing trusted certificate.

For devices using legacy SIM's the following procedure may be used to download the operator root certificate. First, upon sign-up with an operator the customer is required to call a service provisioning number. The operator service center obtains any required information from the customer and starts the certificate download to the device. This download may be accomplished by defining a special SMS message type. Once the procedure is complete the device displays the hash of the certificate and a transaction identifier; hash (certificate/transaction identifier). The hash type used should be the same as that used for the certificate signature. The customer reads this information back to the operator. If this information is correct the provisioning process is complete. Alternative methods to download an operator certificate may be used where appropriate but must insure that the certificate is received by the device unaltered.

Accordingly, a method of operation of a mobile communications device, has been described, comprising: maintaining a list of application programs and, for each application program, a digital fingerprint of that application program; upon execution of an application program, checking the list for an entry that includes the digital fingerprint of the application program, and executing the application program if the digital fingerprint is present; else performing digital signature verification for the application program if the digital fingerprint is not present in the list. Other aspects and embodiments of the invention have been described by way of example only and modifications of detail can be made within the scope and spirit of the invention.

We claim:

Claims

1. A method of operation of a mobile communications device, comprising:

maintaining a list of application programs and, for each application program, a digital fingerprint of that application program;

upon execution of an application program, checking the list for an entry that includes the digital fingerprint of the application program, and executing the application program if the digital fingerprint is present;

else performing digital signature verification for the application program if the digital fingerprint is not present in the list.

2. The method of claim 1, wherein the executing of the application takes place without unconditional verification of a digital signature specific to the application when the digital fingerprint is present.

3. The method of claim 1, further comprising not executing the application program if the digital fingerprint is present in the list but an aging parameter has expired since last occurrence of signature verification for that application program.

4. The method of claim 1, further comprising incrementing or decrementing an aging count parameter upon execution of an application program.

5. The method of claim 1, wherein the step of checking the list comprises generating a digital fingerprint for the application program.

6. The method of claim 1, wherein the method is performed upon downloading of a new application to the mobile communications device.

7. The method of claim 1, wherein the list is maintained in secure memory.

8. The method of claim 6, wherein the list is maintained in a subscriber identity module removeably coupled with the communications device.

9. A communications device comprising:

a first memory storing a list of application programs and, for each application program, a digital fingerprint of that application program;

a second memory for storing application programs;

a digital fingerprint generator for generating a digital fingerprint of an application program prior to its execution;

a digital fingerprint comparator for comparing a digital fingerprint from the digital fingerprint generator with a digital fingerprint from the list and for causing execution of the application program if a successful comparison is made.

10. The communications device of claim 9, further comprising a signature verifier for verifying a digital signature of an application if a digital fingerprint for the application is not present in the list.

11. The communications device of claim 11, wherein the list is stored in a subscriber identity module removeably coupled to the communications device.

12. A method of control of a communications device having a list of digital certificates, comprising:

receiving a certificate configuration message including at least one digital fingerprint of an encoded digital certificate having a digital signature;

comparing the at least one digital fingerprint with a digital fingerprint for a corresponding digital certificate stored in the list of digital certificates and enabling the corresponding digital certificate in the list if there is a successful comparison and disabling the corresponding digital certificate if there is no successful comparison.

13. The method of claim 12 further comprising computing a digital fingerprint for the corresponding digital certificate if there is no digital fingerprint stored in the list when the certificate configuration message is received.

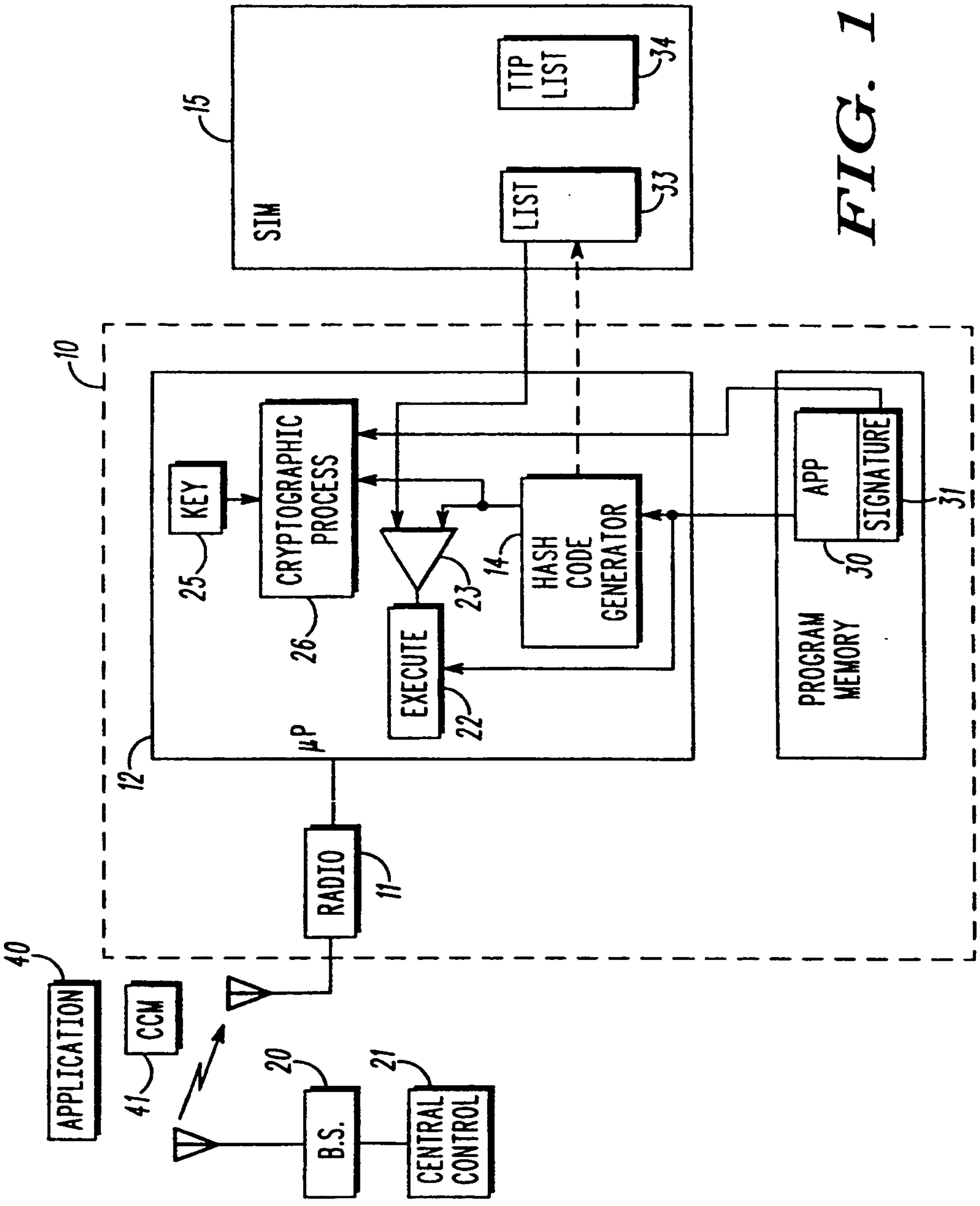

SIM
15
LIST
33
TTP LIST
34
10
12
μP
KEY
25
CRYPTOGRAPHIC PROCESS
26
EXECUTE
22
23
HASH CODE GENERATOR
14
APP
SIGNATURE
30
31
PROGRAM MEMORY
RADIO
11
APPLICATION
40
CCM
41
B.S.
20
CENTRAL CONTROL
21

FIG. 1

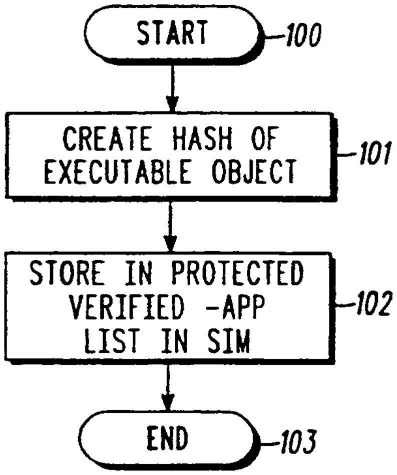

START
100
CREATE HASH OF EXECUTABLE OBJECT
101
STORE IN PROTECTED VERIFIED -APP LIST IN SIM
102
END
103

FIG. 2

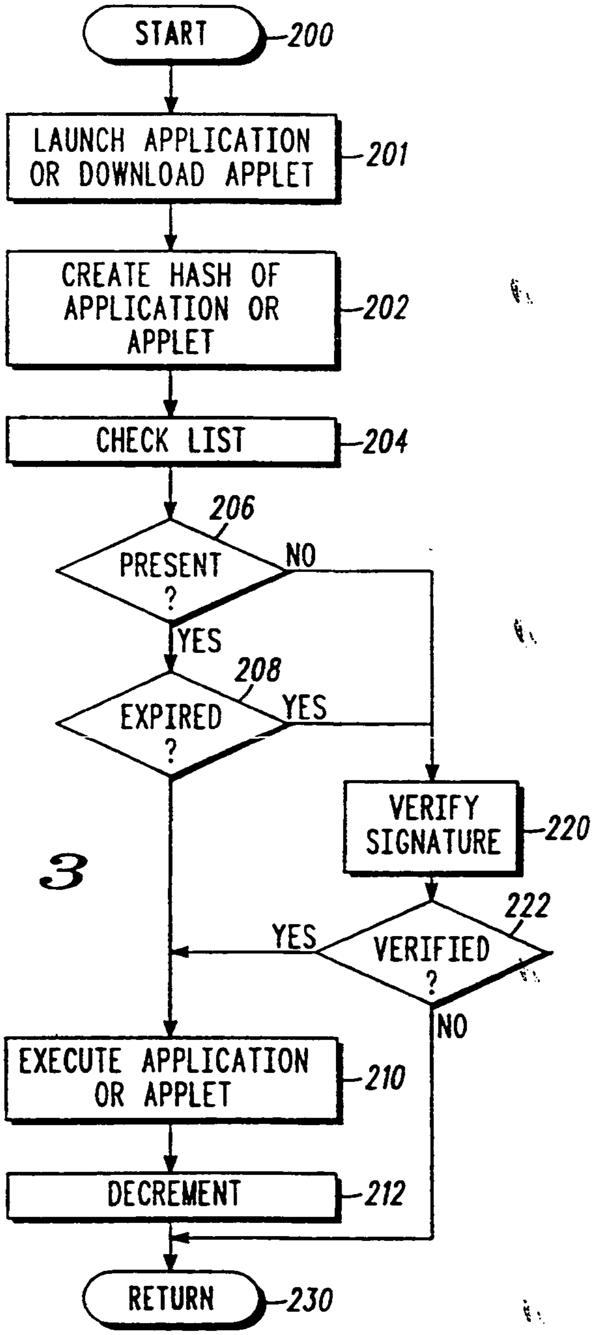

START
200
LAUNCH APPLICATION OR DOWNLOAD APPLET
201
CREATE HASH OF APPLICATION OR APPLET
202
CHECK LIST
204
206
PRESENT ?
NO
YES
208
EXPIRED ?
YES
VERIFY SIGNATURE
220
222
VERIFIED ?
YES
NO
EXECUTE APPLICATION OR APPLET
210
DECREMENT
212
RETURN
230

FIG. 3

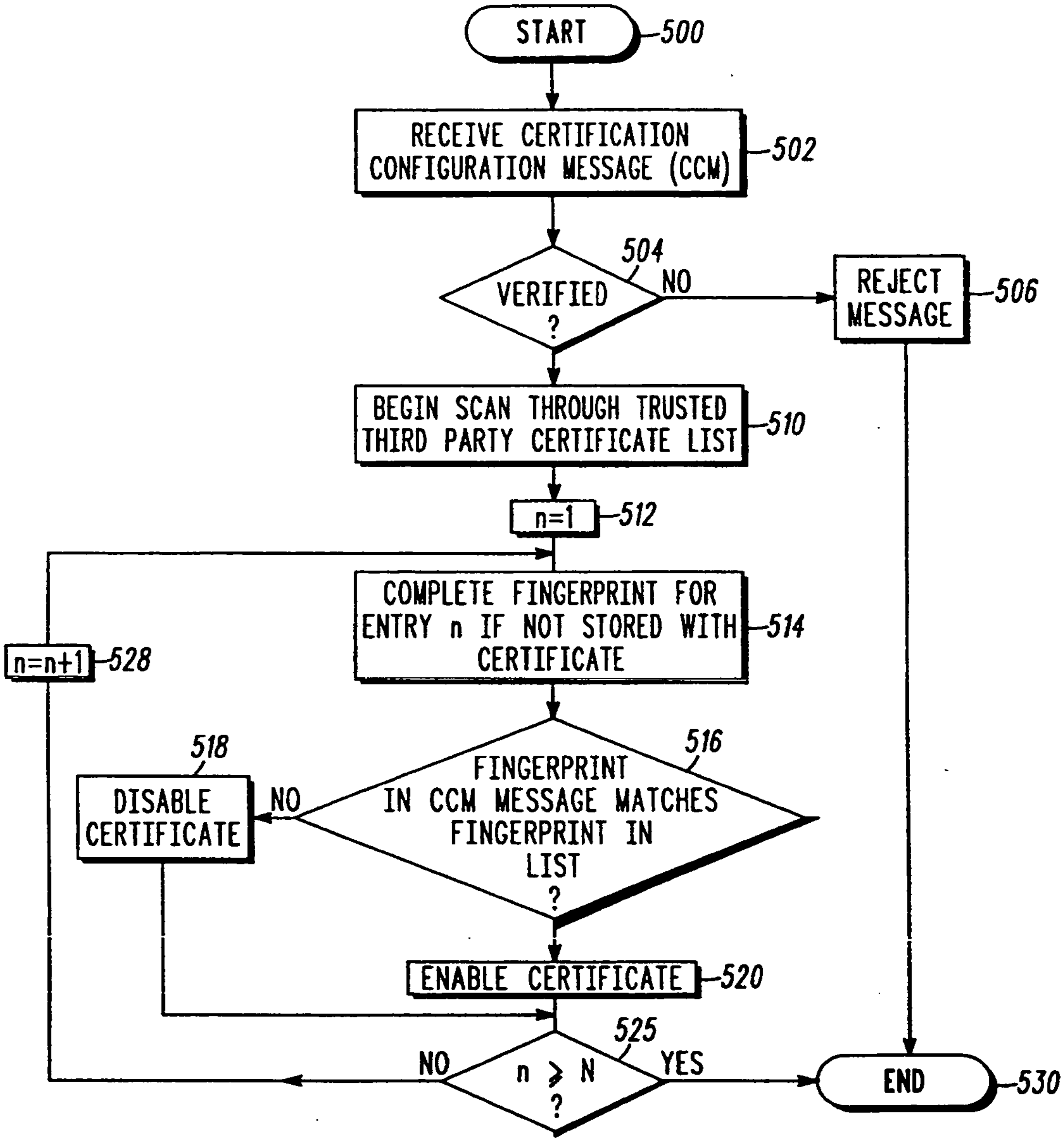

START
500
RECEIVE CERTIFICATION CONFIGURATION MESSAGE (CCM)
502
504
VERIFIED ?
NO
REJECT MESSAGE
506
BEGIN SCAN THROUGH TRUSTED THIRD PARTY CERTIFICATE LIST
510
n=1
512
COMPLETE FINGERPRINT FOR ENTRY n IF NOT STORED WITH CERTIFICATE
514
n=n+1
528
518
DISABLE CERTIFICATE
NO
516
FINGERPRINT IN CCM MESSAGE MATCHES FINGERPRINT IN LIST ?
ENABLE CERTIFICATE
520
525
NO
n ≥ N ?
YES
END
530

FIG. 4

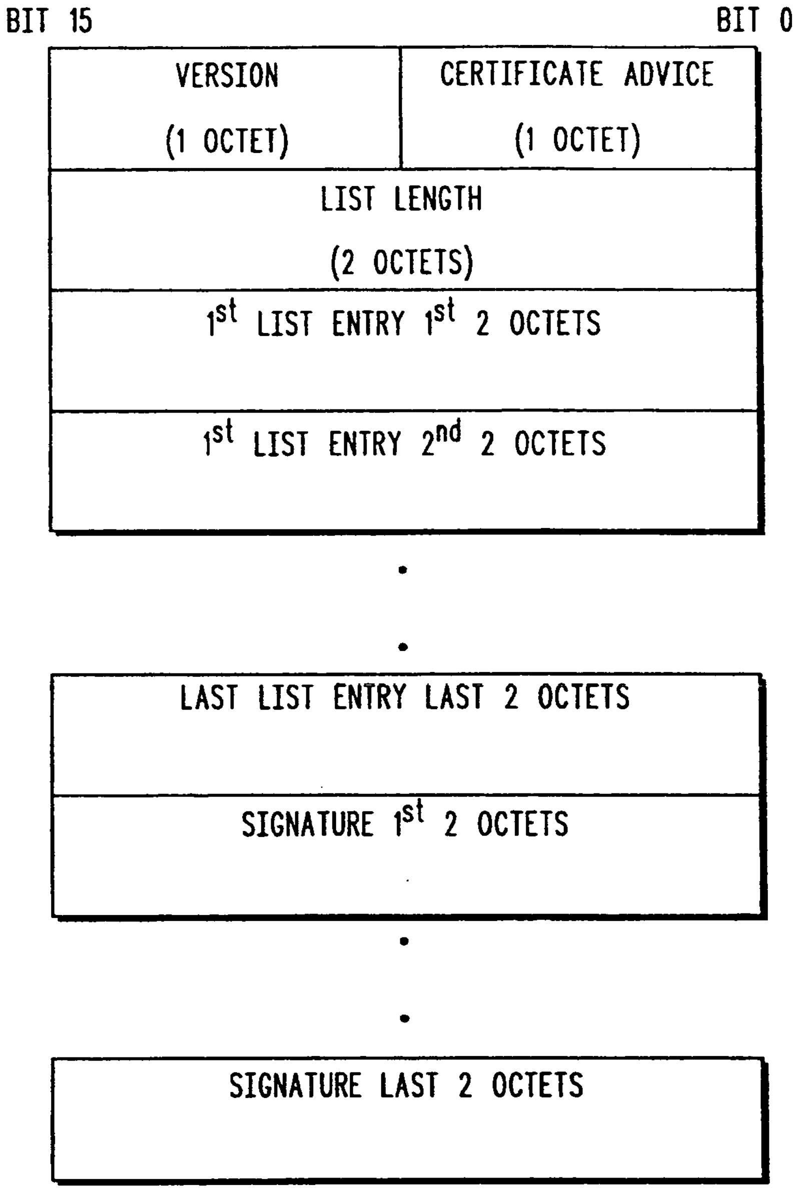

BIT 15
BIT 0
VERSION
(1 OCTET)
CERTIFICATE ADVICE
(1 OCTET)
LIST LENGTH
(2 OCTETS)
1st LIST ENTRY 1st 2 OCTETS
1st LIST ENTRY 2nd 2 OCTETS
LAST LIST ENTRY LAST 2 OCTETS
SIGNATURE 1st 2 OCTETS
SIGNATURE LAST 2 OCTETS

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/11437

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30; H04L 9/00
US CL : 713/187, 158
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/158, 165, 167, 179, 187, 193

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,692,047 A (MCMANIS) 25 November 1997, column 2, line 57; column 9, lines 33-37; column 10, lines 1-15 and 32-35.	1-11
Y	US 5,717,757 A (MICALI) 10 February 1998, column 6, lines 34-38, 51-53, and 61-65; column 7, lines 15-20.	12 and 13
Y	US 5,893,118 A (SONDEREGGER) 06 April 1999, column 9, lines 5-15; figure 2, blocks 42 adn 46.	1-11
Y, P	US 6,021,492 A (MAY) 01 Feburary 2000, column 10, lines 44-65; figure 12.	3 and 4
Y	"Computer Dictionary" Third Edition. Microsoft Press. CIP 1997. Page 228.	1-11

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report
19 JUL 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Gail O. Hayes James R. Matthews
Telephone No. (703) 305-3900